

# Practical Threshold Signatures (1999) (Make Corrections) (95 citations)

Victor Shoup  
Lecture Notes in Computer Science

 [Bookmark in CiteULike](#)



[Home/Search](#) [Bookmark](#) [Context](#) [Related](#)

View or download:  
[shoup.net/papers/thsig.ps.Z](#)

Cached: [PS.gz](#) [PS](#) [PDF](#)

[Image](#) [Update](#) [Help](#)

[Problem Downloading?](#)

From: [shoup.net/papers/ \(more\)](#)  
(Enter author homepages)

Links: [DBLP](#)

([Enter summary](#))

Rate this article: 1 2 3 4 5 (best)

[Comment on this article](#)

**Abstract:** We present an RSA threshold signature scheme. The scheme enjoys the following properties: 1. it is unforgeable and robust in the random oracle model, assuming the RSA problem is hard ([Update](#))

## Cited by: [More](#)

Generic On-line/O-line Threshold Signatures - Chris Crutchfield David ([Correct](#))

Monotone Signatures - Published In Syverson ([Correct](#))

Fast Authenticated Key Establishment Protocols for .. - Huang, Cukier.. (2003) ([Correct](#))

## Similar documents (at the sentence level):

**79.8%:** Practical Threshold Signatures - Shoup (1999) ([Correct](#))

## Active bibliography (related documents): [More](#) [All](#)

**0.2:** On Protocol Security in the Cryptographic Model - Nielsen (2003) ([Correct](#))

**0.1:** A Simplified Approach to Threshold and Proactive RSA - Rabin ([Correct](#))

**0.1:** Why Chosen Ciphertext Security Matters - Shoup (1998) ([Correct](#))

## Similar documents based on text: [More](#) [All](#)

**0.7:** Extracting Witnesses from Proofs of Knowledge in the Random Oracle .. - Groth (2002) ([Correct](#))

**0.4:** Fully Distributed Threshold RSA under Standard Assumptions - Fouque, Stern ([Correct](#))

**0.1:** Using Hash Functions as a Hedge against Chosen Ciphertext Attack - Shoup (2000) ([Correct](#))

## Related documents from co-citation: [More](#) [All](#)

**48:** How to Share a Secret (context) - Shamir - 1979

**29:** A method for obtaining digital signatures and public-key cryptosystems; Communic.. - Rivest, Shamir et al. - 1978

**23:** Random Oracles are Practical: a Paradigm for Designing Efficient Protocols - Bellare, Rogaway - 1993

## BibTeX entry: ([Update](#))

V. Shoup, "Practical threshold signatures", to appear. <http://citeseer.ist.psu.edu/article/shoup99practical.html>  
[More](#)

```
@article{ shoup00practical,
  author = "Victor Shoup",
  title = "Practical Threshold Signatures",
  journal = "Lecture Notes in Computer Science",
  volume = "1807",
  pages = "207--220",
  year = "2000",
  url = "citeseer.ist.psu.edu/article/shoup99practical.html" }
```

## Citations (may not include all citations):

1529 A method for obtaining digital signatures and public-key cry.. - Rivest, Shamir et al. - 1978 [ACM](#) [DBLP](#)

659 Random oracles are practical: a paradigm for designing effic.. - Bellare, Rogaway - 1993 [DBLP](#)